UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/851,625	05/08/2001	Rajasekhar Sistla	42390.P10212	3678

7590 02/09/2006

Edwin H. Taylor
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 Wilshire Boulevard, Seventh Floor
Los Angeles, CA 90025-1026

EXAMINER	
TRUONG, LAN DAI T	
ART UNIT	**PAPER NUMBER**
2143	

DATE MAILED: 02/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/851,625	SISTLA, RAJASEKHAR	
	Examiner	Art Unit	
	lan dai thi truong	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01/10/06*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 May 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim rejections-35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

1) Claims 6-10 and 11-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Leonard et al. (U.S. 6,721,784), herein after referred to as Leonard

In referring to claim 6:

"An input-processing engine to limit abilities of a user of the email client to manipulate an contents of electronic mail received by the email client based on a confidentiality level" (column 9, lines 11-16, 31-37, 46-49). Leonard taught that the sender can control the lifespan of the messages and also can control the electronic mail processing or handling functions such as forwarding, modification, or printing, what means "limit abilities of a user of the email client to manipulate an electronic mail received by the email client based on a confidentiality level."

"An encryption/ decryption engine, coupled to the input-processing engine, to encrypt the electronic mail with authenticated identify information only if the recipient attemps to store the electronic mail to a local storage" (column 21, lines 10-52; column 22, lines 42-44; column 16, lines 55- 67; column 17, lines 32-45). Leonard disclosed method of limiting access electronic

mail messages by storing the files what are equivalent to email folders in encrypted form on the recipient's computer local storage by using recipient's public key. Then the recipient can decrypt those encrypted messages by using his/her private key, So Leonard's ideas may correspond to the limitation of "An encryption/ decryption engine, coupled to the input-processing engine, to limit the user's access to a local storage if the user's access involves an electronic mail"

In referring to claim 11:

" User interface" (column 12, lines 24-33). Leonard disclosed an interface with buttons that permit setting of an expiration date and other handling or processing.

" Communication engine" (column 11, lines 56-67; column 12, lines 1-9, column 14, lines 40-50). Leonard communication engine includes viewer applet, central sever and original software these are equivalent to Communication engine.

" A local storage" (column 21, lines 24-26). Leonard disclosed a local storage for encrypted files.

" An input- processing engine to limit abilities of a user of the email client to manipulate contents of an electronic mail received by the email client based on user-selected confidentiality level" (column 18, lines 66-67;column 19, lines 1-47; column 12, lines 24-33, 54-62).
. Leonard disclosed a method in which the sender can control the lifespan of the messages and also can control the electronic mail processing or handling functions such as forwarding, modification, or printing, what meets the limitation of " to limit abilities of a user of the email client to manipulate an electronic mail received by the email client based on user-selected confidentiality level".

" An encryption/decryption engine, couple to the input processing engine, to encrypt the electronic mail with authenticated identity information only if the recipient attempts to store the electronic mail to a local storage" (column 21, lines 10-52; column 22, lines 42-44; column 16, lines 55- 67; column 17, lines 32-45). Leonard disclosed method of limiting access electronic mail messages by storing the files what are equivalent to email folders in encrypted form on the recipient's computer local storage by using recipient's public key. Then the recipient can decrypt those encrypted messages by using his/her private key.

In referring to claims 7,8:

" The input-processing engine further asserts a first control signal to disable options that are originally supported by the email client if the confidentially level satisfies a predefined confidentiality threshold. Wherein the first control signal is a confidentiality-level-dependent control signal" (column 16, lines 12-25; column 19, lines 7-12; column 22, lines 37-44; column 24, lines 10-38). Leonard disclosed the message header is the field for including control information such as flags what means asserting a confidentiality-level-dependent control signal used to enable or disable options what are originally supported by the recipient for electronic mail processing or handling functions such as printing, coping, or forwarding.

In referring to claim 9:

" The input-processing engine further asserts a second signal to invoke the encryption/decryption engine in response to the user's access" (column 13, lines 56-62; column 20, lines 66-67; column 21, lines 1-52; column 22, lines 42-44; column 16, lines 55-67; column 17, lines 32-45). Leonard taught that after being asked to supply the identity information to identify member of affinity group for enroll into privacy email system, which is shared identical

functionality with asserting second signal, recipient can either store message in encrypted form or decrypt those message from recipient's computer local storage, then recipient can decrypt those encrypted messages by using his/her private key.

In referring to claim 10:

" The encryption/ decryption engine further prompts the user for identity information" (column 13, lines 56-62). Leonard disclosed method of opt-out and opt-in what are shared identical functionality with providing authenticating identity information.

"If the user's access to the local storage is to store the electronic mail, encrypts the electronic mail with the identity information; and if the user's access to the local storage is to retrieve the electronic mail, decrypts the electronic mail with the identity information" (column 21, lines 10-52; column 22, lines 42-44; column 16, lines 55- 67; column 17, lines 32-45). Leonard disclosed method of limiting access electronic mail messages by storing the files what are equivalent to email folders in encrypted form on the recipient's computer local storage by using recipient's public key, what means "If the user's access to the local storage is to store the electronic mail, encrypts the electronic mail with the identity information". Then the recipient can decrypt those encrypted messages by using his/her private key, what means "if the user's access to the local storage is to retrieve the electronic mail, decrypts the electronic mail with the identity information"

In referring to claim 12:

"wherein the user interface further comprises: First set of confidentiality levels for the user to select from; and a second of options to manipulate the electronic mail for the user to select from" (column 18, lines 66-67;column 19, lines 1-47; column 12, lines 24-33, 54-62).

Leonard disclosed a user interface includes the message screen, menus window and function bars to manage and enable use of features of electronic mail what is share identical functionality with set of confidentiality levels and options to manipulate the electronic mail for the user to select from.

In referring to claims 13,14:

" Wherein the electronic mail confidentiality preserver further asserts a first control signal to the user interface to disable selected options from the second set of options if the confidentiality level satisfies a predefined confidentiality threshold. Wherein the first control signal is a confidentiality-level-dependent control singal" (column 16, lines 12-25; column 18, lines 66-67;column 19, lines 1-47; column 22, lines 37-44; column 24, lines 10-38). Leonard disclosed the message header is the field for including control information such as flags what refer to asserting a control signal which is equivalent to confidentiality-level-dependent control signal used to enable or disable options what are originally supported by the recipient for electronic mail processing or handling functions such as printing, coping, or forwarding.

In referring to claim 15:

" The input-processing engine further assert a second control signal to invoke the encryption/decryption engine in response to the user's access" (column 13, lines 56-62; column 20, lines 66-67; column 21, lines 1-52; column 22, lines 42-44; column 16, lines 55-67; column 17, lines 32-45). Leonard taught that after being asked to supply the identity information to identify member of affinity group for enroll into privacy email system, which is shared identical functionality with asserting second signal, recipient can either store message in encrypted form

or decrypt those message from recipient's computer local storage, then recipient can decrypt those encrypted messages by using his/her private key.

In referring to claim 16:

" The encryption/ decryption engine further prompts the user for identify information" (column 13, lines 56-62). Leonard disclosed method of opt-out and opt-in what are shared identical functionality with providing authenticating identity information.

" If the user's access to the local storage is to store the electronic mail, encrypts the electronic mail with the identification, and if the user's access to the local storage is to retrieve the electronic mail, decrypts the electronic mail with the identify information" (column 21, lines 10-52; column 22, lines 42-44; column 16, lines 55- 67; column 17, lines 32-45). Leonard disclosed method of limiting access electronic mail messages by storing the files what are equivalent to email folders in encrypted form on the recipient's computer local storage by using recipient's public key what means "If the user's access to the local storage is to store the electronic mail, encrypts the electronic mail with the identity information". Then the recipient can decrypt those encrypted messages by using his/her private key, what means "and if the user's access to the local storage is to retrieve the electronic mail, decrypts the electronic mail with the identity information".

Claim rejections-35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or descry

bed as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2) Claims 1-5 and 17-21 are rejected under 35 U.S.C 103(a) as being un-patentable over Leonard et al. (U.S. 6,721,784) in view of Marvit et al. (U.S. 6,625,734)

In referring to claim 1:

"Authenticating identity information of the recipient" (column 13, lines 56-62). Leonard disclosed method of opt-out and opt-in what are shared identical functionality with providing authenticating identity information of the recipient.

" Restricting the recipients ability to manipulate contents of the electronic mail based on the confidentiality level established by the sender" (column 9, lines 11-16, 31-37, 46-49). Leonard disclosed a method in which the sender can control the lifespan of the messages and also can control the electronic mail processing or handling functions such as forwarding, modification, or printing, what meets the limitation of " Restricting the recipients ability to manipulate the electronic mail based on the confidentiality level established by the sender".

" Encrypting the electronic mail with the authenticated identity information only if the recipient attempts to store the electronic mail to a local storage: (column 21, lines 10-52; column 22, lines 42-44; column 16, lines 55- 67; column 17, lines 32-45). Leonard disclosed method of limiting access electronic mail messages by storing the files what are equivalent to email folders in encrypted form on the recipient's computer local storage by using recipient's public key

However, Leonard does not explicitly discloses method of and decrypting the electronic mail only if the recipient attempt to retrieve the electronic mail from the local storage

Marvit discloses method of decrypting encrypted messages from user local storage if the user wishes to read them: (column 16, lines 48-57)

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Marvit's ideas of decrypting encrypted messages from user local storage with Leonard's system in order to provide security system

In referring to claim 2:

" Where the identity information is a system password" (column 13, lines 56-62). Leonard-Marvit disclosed method of opt-out and opt-in means password providing.

In referring to claims 3 and 19:

" Prompting a user of the recipient to supply the identity information; decrypting the electronic mail with the identity information supplied by the user" (column 13, lines 55-62; column 14, lines 45-46, 56-67; column 16, lines 55-67, column 17, lines 32-44). Leonard-Marvit taught that after being asked to supply the identity information such as password from recipient to identify member of affinity group, what means "prompting a user of the recipient to supply the identity information", then the recipient can receive encrypted message for message viewing by using the viewer applet what is installed in recipient's computer what have ability to decrypt the encrypted message to view, what means "decrypting the electronic mail with the identity information supplied by the user"

In referring to claims 4,5:

" asserting a control signal to disable options that are originally supported by the recipient if the confidentiality level satisfies a predefined confidentiality threshold, wherein the control signal is a confidentiality-level-dependent control signal" (column 16, lines 12-25; column 19, lines 7-12; column 22, lines 37-44; column 24, lines 10-38). Leonard-Marvit disclosed the message header is the field for including control information such as flags what means asserting a confidentiality-level-dependent control signal used to enable or disable options what are originally supported by the recipient for electronic mail processing or handling functions such as printing, coping, or forwarding.

In referring to claim 17:

"Authenticating identity information of the recipient of an electronic mail" (column 13, lines 56-62). Leonard disclosed method of opt-out and opt-in what are shared identical functionality with providing authenticating identity information.

" Restricting the recipients ability to manipulate contents of the electronic mail based on the confidentiality level established by the sender of the electronic mail" (column 9, lines 11-16, 31-37, 46-49). Leonard disclosed a method in which the sender can control the lifespan of the messages and also can control the electronic mail processing or handling functions such as forwarding, modification, or printing, what meets the limitation of "Restricting the recipients ability to manipulate the electronic mail based on the confidentiality level established by the sender of the electronic mail".

" Encrypting the electronic mail with the authenticated identity information if the recipient attempts to store the electronic mail to a local storage: (Leonard disclosed method of limiting access electronic mail messages by storing the files what are equivalent to email folders

in encrypted form on the recipient's computer local storage by using recipient's public key: column 21, lines 10-52; column 22, lines 42-44; column 16, lines 55- 67; column 17, lines 32-45)

However, Leonard does not explicitly discloses method of decrypting the electronic mail only if the recipient attempt to retrieve the electronic mail from the local storage

Marvit discloses method of decrypting encrypted messages from user local storage if the user wishes to read them: (column 16, lines 48-57)

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Marvit's ideas of decrypting encrypted messages from user local storage with Leonard's system in order to provide security system

In referring to claim 18:

" Where the identity information is a system password" (column 13, lines 56-62). Leonard disclosed method of opt-out and opt-in what is password providing.

16) In referring to claim 19: " Prompting a user of the recipient to supply the identity information; decrypting the electronic mail with the identity information supplied by the user" (column 13, lines 55-62; column 14, lines 45-46, 56-67; column 16, lines 55-67, column 17, lines 32-44). Leonard-Marvit taught that after being asked to supply the identity information such as password from recipient to identify member of affinity group, what means "prompting a user of the recipient to supply the identity information," then the recipient can receive encrypted message for message viewing by using the viewer applet what is installed in recipient's computer what have ability to decrypt the encrypted message to view, what means "decrypting the 13electronic mail with the identity information supplied by the user".

In referring to claim 20, 21:

" asserting a control signal to disable options that are originally supported by the recipient if the confidentiality level satisfies a predefined confidentiality threshold, wherein the control signal is a confidentiality-level-dependent control signal" (column 16, lines 12-25; column 19, lines 7-12; column 22, lines 37-44; column 24, lines 10-38). Leonard-Marvit disclosed the message header is the field for including control information such as flags what refer to asserting a control signal which is equivalent to confidentiality-level-dependent control signal used to enable or disable options what are originally supported by the recipient for electronic mail processing or handling functions such as printing, coping, or forwarding.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to lan dai thi truong whose telephone number is 571-272-7959. The examiner can normally be reached on monday- friday from 8:30am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Lan Dai Thi Truong
Examiner
Art Unit 2143

Ldt
02/01/2006

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100